Privacy Impact Assessment (PIA)

BioConnect: combining facial recognition and MAC address tracking for authorising access to Wi-Fi

Stuart Millar 13616005

Email: smillar09@qub.ac.uk

15th November 2016

Table of Contents

Introduction

Privacy Impact Assessments (PIAs) are documents that help organisations identify the most effective way to comply with data protection obligations, such as the Data Protection Act 1998 (DPA), and meet expectations of privacy held by individuals. By highlighting risks and proposing solutions at an early stage, PIAs help reduce damage to a firm's reputation, legal action, financial penalties and other costs incurred through the triggering of potential scandals. The purpose of the PIA is to ensure that privacy risks are minimised while allowing the aims of the project to be met whenever possible.

This document first sets out the need for a PIA in more detail along with information flows for the BioConnect system. Our consultations with various stakeholders are then discussed before outlining the risks and proposed solutions for the system. Lastly our PIA outcomes propose which of the solutions should be implemented and how the project should be managed to address risks now and in the future.

As per the Information Commissioner's Office (ICO) PIA code of practice [1], conducting a PIA produces better policies and systems, and improves relations between organisations and individuals. A PIA enables an organisation to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved. These risks, such as those causing distress to individuals, or impacts of a datastore being compromised, are identified by analysing how the proposed uses of personal information and technology will work in practice. Our analysis also included privacy concerns gathered after consulting stakeholders who will be working with, or be affected by, the project.

Privacy

The higher the risk level - and the more intrusive the project - the higher the impact on privacy. We can say privacy is the right of the an individual to be left alone [1]. This can be physical privacy, where a person wants their own personal space without intrusion and searches, or informational privacy, where a person controls, edits, manages and deletes information about themselves, plus decides how much of that information is shared with others. Intrusion in the informational sense may regard disclosure without consent or collecting too much information on an individual. Article 8 of the Human Rights Act 1998 [2] concerns the right to respect for private and family life.

Privacy risk, which this PIA seeks to minimise, is the risk of harm arising through an intrusion into privacy. It can be obvious, like financial loss. It can also be less defined, like identify theft, breakdown of relationships or negative effects on society in the wider sense, such as a perceived loss of personal autonomy.

BioConnect Background

BioConnect is a new Internet of Things (IoT) product that uses a combination of facial recognition and a mobile phone MAC address tracking for authorising access to Wi-Fi. The system requires user consent to access the Wi-Fi unless they have already given their consent via previous use. The Wi-Fi network will be provided by BioConnect. It is envisaged BioConnect is most beneficial in three main areas: large public, private or hostile environments, on travel networks and at home. The terms 'phone' and 'device' are interchangeable from this point on. Example usage:

- In the home for controlled Wi-Fi access to prevent unauthorised use of devices, for example by children.
- In public places to reduce device theft and help catch thieves.
- Across a regional or international travel network incorporating subways, buses, train stations, airports and such like. It may be particularly useful for helping to secure large travel networks which may under terrorist threat, like the London Underground.
- Locating individuals under some kind of time pressure, for example those who are late for a flight, or in more severe circumstances trying to pin-point terrorists inside a building where hostages are being held.
- In retail stores for tracking customer movements.
- In buildings for tracking who is inside, and thus who is not.
- For specific surveillance e.g. on travel networks, sports stadiums, entertainment parks, universities, schools, workplaces, supermarkets, conferences and events with controlled access, for example via turnstiles. This helps reduces risks of crime and terrorist attacks in venues and environments with a high density of people.

In order to join a Wi-Fi network, the system requires a picture of the user's face. The first time a user joins a network, this is stored with the MAC address of the device attempting to access the Wi-Fi. Consider a MAC address to be a unique ID for each phone. Once a facial image and MAC address are recorded for a given device, the next time access is attempted, the image of the user must match the original capture. When a user returns to an environment where they have previously used the Wi-Fi and requests access once more, the system will check their face against the stored picture, and if the device MAC address matches the stored MAC address, then Wi-Fi access will be granted.

In a home situation for example this prevents children using parent's devices. In other environments, if required, it is possible to alert an authority if a previously registered device attempts access and the image of the individual does not match that which is stored. This authority could be an on-site administrator, or a security team. In environments where the datastore is shared with official security services, they can be notified also, for example if a known criminal or terror suspect is identified.

In most cases it is thought the camera in the device attempting access will be used to take the picture. Alternatively, it can be taken via the installed cameras in the environment. For example, a camera in a user's house, or via a special kiosk camera in public, or cameras installed in the back of seats on a train.

The system can track users in an environment via their MAC address. People can also be tracked via their facial image. For example, in an airport if a connected device is stationary for an abnormal period of time, security can be notified and it can be investigated. The MAC address allows the specific model of device to be identified. Samsung Galaxy Note 7 devices, which at time of writing are vulnerable to catching fire, have been banned by the US Department of Transportation from being carried onto a plane either in hand luggage or checked-in luggage.

The Need for a PIA

The ICO created a set of screening questions to help identify when a PIA is needed [1]. We begin by analysing the project using these questions, and if any of the answers are 'yes', then we can say a PIA is strongly recommended. What follows are each of the questions and the answers pertaining to BioConnect.

Will the project involve the collection of new information about individuals?

Yes. BioConnect will collect facial recognition images of individuals and mobile phone MAC addresses of the devices that they are using. This is new information which is not already available to us as a company.

Will the project compel individuals to provide information about themselves?

Yes. To use the service, individuals will be compelled to provide information about themselves. It is proposed a facial recognition image is required along with their device's MAC address.

Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?

Yes, in certain circumstances. The facial recognition images and MAC addresses may be shared or pooled with security services depending on the implementation of the product and we will be obliged to assist with investigations relating to, for example, national security or prevention of crime.

Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?

Yes. We are not aware of widespread installations of a system that uses a combination of facial recognition and mobile phone MAC address tracking in order to grant access to a Wi-Fi network. Separately, facial recognition technology already exists, as does the ability to track mobile phone locations via MAC addresses within a local network.

Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.

Yes. We appreciate that facial recognition could be viewed as intrusive. The technology is not common in the environments that we are proposing, for example at home and in public places.

Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?

Yes. These decisions and actions taken vary in severity. If a potentially stolen device attempts to access the Wi-Fi network and the facial recognition image does not match that which is stored, the security team in a given environment may be notified depending on the protocol of that environment. More serious cases such as identifying wanted criminals and preventing terrorism may mean official law enforcement officials are involved leading to possible cautions or arrests.

Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.

Yes. The information centres on tracking and identifying individuals. Provided the required data exists and has not been deleted, at a given point in time it will be possible to build a picture of which Wi-Fi networks a device has used over a set period of time, and hence where that same user has been, by filtering the datastore to search for a given MAC address or given facial recognition image.

Will the project require you to contact individuals in ways which they may find intrusive?

No. There is no intended functionality in this product to contact individuals via their device, which could be considered intrusive, or via any other intrusive manner. However, if this changes then we will certainly need to evaluate this and conduct another PIA accordingly, for example if some sort of alerts need sent to a device in the event of a Wi-Fi breach or some other security event.

Information Flows

This section explains how the information in the BioConnect system is obtained, used and retained. In other words, what information is used, what it is used for, who it is obtained from and disclosed to, who will have access and any other necessary information. It also details how it is collected, used, deleted and how many individuals are affected. Here, we have used an adaptation of data mapping and information flow similar to that used in the NHS [3], as it was felt it fitted well with the semantics of this project. To begin with, we can describe the source and justification of collecting the data involved:

1. Facial recognition image from phone

Source: The user's device. The image is taken with their camera and is uploaded to the system server when requested.

Justification: Needed for access to Wi-Fi. If an image already exists on the system for a user, then they do not need to upload another image. Tightens security by preventing other people using that same device to access Wi-Fi. At home, prevents unauthorised use of devices, for example by children. Helps identify known criminals or suspects who are using the Wi-Fi service and so are present in the area.

2. Facial recognition image from installed IoT camera

Source: An installed IoT camera.

Justification: Once a user's device requests to re-join a network they have used before, the IoT camera automatically takes a facial recognition image and checks it against that held in the datastore. If they match, and the MAC addresses match, then access is granted. This process speeds up both re-joining a Wi-Fi network and the rejection of access also. We can track by facial recognition as well.

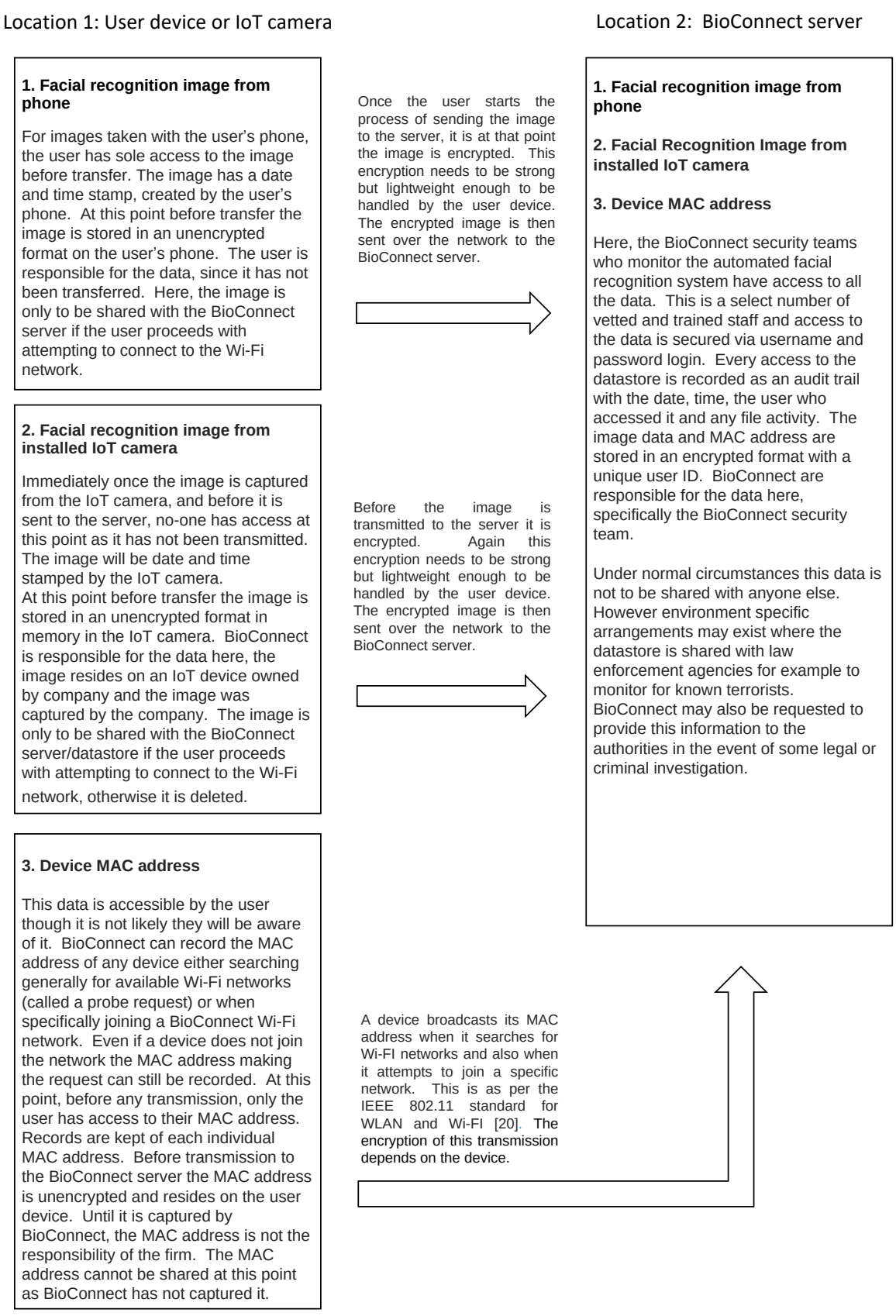
3. Device MAC address

Source: Any device which attempts to access the network, the source is the device itself.

Justification: Used in conjunction with the facial recognition. If both match a previously held record, then access is granted. On first-time use this is stored with the facial recognition image, effectively forming a record for a user. The MAC address allows us to detect what phone models are being used and if any banned devices are in use. We can also track a MAC address in the Wi-Fi network at the same time as facial recognition, which lets us report abnormal behaviour, such as suspect devices being stationary, or if a user path deviates abnormally from the MAC address path.

Next, the flow of the information can be studied in Figure 1 below. This includes details of who has access to the data, audit trails, the format and storage of the data, who is responsible for it, if it is to be shared, and how the data is transferred between points of rest. Depending on the nature of the system usage, the information for only half a dozen users could be stored, or it could run to hundreds of thousands or millions.

Figure 1 - BioConnect information flow between points of rest



Consultation

Consultation is a crucial part of the PIA which lets internal and external stakeholders highlight privacy risks, and sometimes solutions, based on their own specialist area.

Four stakeholders were selected for consultation and below are descriptions of their profiles, why they were selected and why they were asked the questions chosen.

The full questionnaires for each stakeholder along with their answers can be found in Appendix A.

- *Stakeholder 1* is a home-owning female parent, 40 years-old, with two children under the age of 10 years-old. They have various devices at home that could use this system though this stakeholder is not particularly tech-savvy. Also, they use public transport regularly both on their own and sometimes bring their children. This gave a family viewpoint and concerns parents would have. Overly technical responses from them were not the aim, rather we wanted concerns that are more likely to be held by the public at large, who used Wi-Fi occasionally on the move, but for whom their family and their personal safety were the priorities.

- *Stakeholder 2* is a senior business executive that travels internationally daily by air and by train. When they travel they also use their laptop, tablet and mobile device for business use and personal use. We chose a businessman to get an idea of concerns of someone who travels regularly and would be subject to heightened security procedures in places such as airports or train stations, and who may be concerned about their business data being compromised by using Wi-Fi outside the relative safety of their office. Also, we assert a businessman on the move is time poor and we were interested in how much attention would be paid to terms of service for Wi-Fi and if BioConnect may make them feel safer when travelling given terrorist threats.

- *Stakeholder 3* sits on the internal cyber security committee of BioConnect. They previously were an ethical hacker and worked as a contractor to strengthen vulnerable systems. From time to time they also appear as a guest in the media to discuss cyber security incidents. This stakeholder was chosen to use their experience commentating on negative incidents in the press to get opinion on how the media would react to an unfavourable situation. We also wanted comparison with similar projects to see if there is a risk of BioConnect being unreasonable with the data collection for this project. Given their background we could also gain some extra insight into technical mitigations.

- *Stakeholder 4* is a 23-year-old tech savvy university student living in London. They are something of a fair-weather protester with regard to privacy and human rights but they are still important to this stakeholder, and they attend rallies when they can. They've been the victim of phone theft in the past and their parents were caught up in the London Underground bombing in 2005, although they were not harmed. There are large parts of society that are more privacy sensitive than others, and we wanted a stakeholder in this group who had been affected negatively in the past by an incident that could be prevented in future by the BioConnect system. Selecting a student may give more emotional answers to highlight potential risks given the fact they are more opinionated, and possibly more frank, than other stakeholders.

Risk Analysis & the Risk Register

We considered a significant amount of legislation, regulations, codes of practice and previous scandal when building the Risk Register. In this section we consider each of these areas and add in the concerns gathered from the consultation to create a final Risk Register that can be seen in Table 1, complete with color-coding for severity.

The following legislation and regulations were studied:

- Data Protection Act 1998 [5]
- Human Rights Act 1998 [2]
- Draft Investigatory Powers Bill 2015 [7]
- European General Data Protection Regulation [9]
- Lawful Business Practice Regulation 2000 [10]
- The Regulation of Investigatory Powers Act 2000 [12]
- Privacy and Electronic Communications Regulations PECR [13]

Data Protection Act 1998 [5]

Let us consider the Data Protection Act 1998 first, and whether personal data is used by BioConnect or not. The data described in the information flows for BioConnect is clearly electronic data, which is one of the four data types the DPA concerns itself with [4, 5]. On its own, a MAC address cannot identify an individual. However, when we process it, and track it, then we learn something about the individual using that device, and we can say the data potentially could impact an individual in a personal, or business or professional capacity. Facial recognition images are obviously about an individual as we are all unique inherently. When we combine a facial recognition image and a MAC address, and then store this record with a unique ID, there is no doubt this is personal data for the purposes of the DPA. This is also sensitive personal data as we may be able to tell race and ethnicity from the images.

We can consider each of the eight principles of the DPA and if BioConnect is at risk of violating them. For brevity we have not included the wording here in full, the DPA principles can be found in Appendix B.

Principle 1 – we can fairly and lawfully process this data once the data subject has given his consent to processing. In some cases, like a hostile environment or high security situations, the processing is necessary to protect the vital interests of the data subject and would be necessary for the exercise of a related function of a government security department. Since it is sensitive data, the data subject must give explicit consent to the process, or - in theory - we can process the data if consent was withheld, say in a high security or hostage situation. We must be transparent that we are processing this data and we must get explicit consent when a user first gains access. It must be considered how a user withdraws consent and the mechanism for this needs to be made clear when they sign-up.

Principle 2 – it must be specified what the data is being obtained for and it must not be processed further than for that purpose. Controlling potential new purposes of data is needed. Not doing so could lead to discrimination or abuse of data, like gathering shopping or travel habits.

Principle 3 – we are sure the data collection is not excessive. BioConnect provides secure Wi-Fi and using a phone's MAC address and a facial recognition image instead of, say, a username and a password, is adequate, relevant and the minimum required. It is not possible to implement the project without these.

Principle 4 – the data must be accurate and kept-up to date, bearing in mind if on occasion a user buys a new phone or if a device is sold as second hand device.

Principle 5 – the data must not be kept longer than needed.

Principle 6 – handling Subject Access Requests are important. An example of poor handling of SARs would be not handling them in time.

Principle 7 – appropriate technical and organisational measures have to be in place. Facial recognition images and MAC addresses have to be protected. They could be hacked in transmission. Insider threats are an issue.

Principle 8 – regarding the transfer of personal data, certain implementations of BioConnect may sit outside the EEA. Countries outside the EEA may not enforce equivalent law and regulations as in the UK.

Human Rights Act 1998 [2]

BioConnect is not a core public authority. However, in certain circumstances, we are required to act in line with the Human Rights Act 1998 (HRA), as we can be said to exercise a "function of a public nature". Provision of Wi-Fi to potentially thousands of users in public spaces is clearly public in nature. We feel security makes people feel safer, it is a social need, intrinsic to human beings. As per Article 8 of the HRA, we respect everyone's private and family life, home and correspondence. BioConnect does not compel anyone to use it and consent can be withdrawn.

Draft Investigatory Powers Bill (DIPB) 2015 [7]

This bill almost certainly will become law before the end of 2016 [8] and needs consideration. BioConnect can be seen as a Communications Service Provider (CSP) in the eyes of this bill. Hence it is required that for 12 months we store the websites a user visits, though not the individual pages. This requirement applies to all the other CSPs operating in the UK too. BioConnect will be bound by this bill and will need to work with the police and authorities as needed. Our attitude will be to set the best example possible if our help is required. The Data Retention (EC Directive) Regulations 2009 [14] also has a similar stipulation to keep data for 12 months from the date of communication.

European General Data Protection Regulation (EGDRP) [9]

We need to be compliant with this in future when it is introduced in May 2018. There is something of a conflict with the DIPB in that it increases power of the authorities in the UK whilst the EGDRP increases civilian power instead. The EGDRP also requires PIAs to be undertaken, and is likely to be strongly against compulsory use of biometrics.

Lawful Business Practice Regulation 2000 [10]

This regulation applies to BioConnect if it is implemented in the workplace. It allows monitoring and recording of communications in the interest of national security and to prevent and detect crime.

The Regulation of Investigatory Powers Act 2000 [12]

Perhaps surprisingly this Act allows agencies like the Environment Agency or the Food Standards Agency to use investigatory powers, not just well known national security services. It could be said their application of the powers may not be as stringent as security services, so vigilance is needed.

Privacy and Electronic Communications Regulations (PECR) [13]

These are extra rules that sit alongside the DPA and apply to any electronic communications service that is provided so as to be available for use by members of the public, such as BioConnect. Similar to the DPA principle 7, measures must be taken to secure BioConnect and customers should be informed of the risks. It also reminds us tracking location data requires consent, and there needs to be procedures for responding to other bodies who ask for personal data. The ICO can check these procedures too.

Other codes of practice & industry codes of conduct

ICO guidance [6] states the use of surveillance systems for limited household purposes can be exempt from the DPA. Still, it is sensible to take home use as seriously as other environments. It points out that disclosing surveillance images of an individual, such as those generated by BioConnect, may intrude on others privacy if they are in the background. [6] points out the ability to obscure the background of images is ideal and that staff should be appropriately trained. Also, once information is disclosed to a 3rd party, they become responsible for the copy of the data they hold. However, BioConnect could still get a negative public reaction if the 3rd party mishandles the information. [6] also recommends carrying out a PIA and adhering to Privacy by Design (which we shall discuss later) when there is a chance that personal data will be pooled into big data systems, and states that automated recognition technologies attract the same data protection concerns. They say the matching process should not be 100% automated, and recommend the results of automated matching should be monitored by trained individuals to ensure there haven't been mismatches.

The ICO have also produced Wi-Fi location analytics guidance [16] which reinforces the fact that a MAC address can become personal data if combined with other information. In the case of BioConnect this other information comprises facial recognition images. It explains that probe requests from user devices when searching for a network (and before one is even joined) can have the MAC addresses extracted and stored. This can be seen as unnecessary collection of personal data if the user is not providing a facial recognition image as well to ultimately join the Wi-Fi network.

Consideration of relevant IoT & surveillance scandals

We need to be aware of the risk of false positives being generated by BioConnect. For example, in the 2001 Superbowl, facial biometrics were used to identify criminals, but twelve false positives (or false alarms) were generated. There was a scandal where smart bins monitored the MAC addresses of mobile phones in London, and showed targeted content via advertising screens on the bins. These were banned by the City of London and is a good example of transparency being needed to reduce possible negative reaction. We can also consider the Nordstrom scandal, were they left it too late to inform customers they were tracking how customers navigated their stores, which resulted in negative press. Big Brother Watch [11], a privacy rights campaign group, can also cause negative reactions with their challenges to law and policy along with public revelations about surveillance.

Concerns uncovered through the consultations

The consultations were useful in highlighting privacy risks and these were added to the Risk Register, referenced by used of (R*x*) where *x* is a number.

Stakeholder 1 – home owning female parent with children

- Concerned that the Wi-Fi network itself has to be secure so sensitive data like banking information and photos can't be compromised (R7).
- Worried about the system tracking her location and storing pictures of her or her kids – so clarification is needed in the T&Cs, clear signage is needed, and explain the system is there for security and safety. Again do not compel users to to use it (R1).
- The positioning of the cameras could be intrusive. But at the same time, they cannot be covert (R18).
- Feels there is a risk sensitive pictures could be sent (R19). Highlights the need not to compel people to use it, to be wary of data sharing, disclosure and unnecessary data.
- Felt it was better to store data in the office rather than the cloud (R7).
- Highlighted physical risk of being attacked by a criminal (R20)
- They probably wouldn't read the T&Cs (R1).

Stakeholder 2 – business man who travels regularly

- Also concerned about the transmission of data, again concerned that the Wi-Fi network has to be secure (R7).
- Gave some validation to using BioConnect to track banned devices going onto planes, being "ok" with that data being stored but nothing extra, and expressed concern about too many photos being stored (R4, 5, 17, 19).
- Wanted to be able to have info deleted on request and view / edit what was being stored about them (R1).
- Concerned about tracking data being revealed publically and harming commercial relations (R5).
- Also probably wouldn't have time to read T&Cs (R1).

Stakeholder 3 – internal member of BioConnect cyber security committee

- Raised concerns about success in identifying falsified facial images (R21).
- Recommended high-quality cameras be used but pointed out differences in mobile phone cameras compared to the installed cameras, and spoofing of MAC addresses (R22).
- Also raised concerns about device constraints of IoT and their vulnerabilities (R7).
- Suggested use of Role Based Access Control (RBAC) (R8).

Stakeholder 4 – tech savvy student who has been a victim of theft and whose parents were caught up in a terrorist attack

- Concerned about personally sensitive info (R1).
- Concerned about being able to delete information (R4, 5, 17, 19).
- Raised prospect of blurring background images of people (R15).
- Not comfortable with location tracking (R17).
- Concerned about identifying faces also, i.e. false alarms (R21).
- Concerned about insider threats, staff suitability (R8), how data is updated (R4) and stored (R7).
- Feels that storing names and dates of birth are unnecessary, and after consideration we agree.

This stakeholder also made an interesting point about storing the list of vulnerable devices and checking a phone's MAC address against that, rather than storing all the phone's MAC addresses. This idea could be developed further in future. They suggested too that the authorities should provide the criminal facial images for BioConnect to check against, instead of requesting access. This is useful but we doubt it would be possible legally for the authorities to do that.

Table 1 – The Risk Register

Risk ID	Privacy Issue	Risk to Individuals	Compliance Risk	Associated Corporate Risk	Likelihood	Severity
R1	Obtaining Explicit Consent / Awareness	Unauthorised data processing	DPA Principle 1	Reputational damage, loss of public trust and legal action.	High	High
R2	Withdrawing Explicit Consent	Unauthorised data processing and data not being deleted	DPA Principle 1	Reputational damage, loss of public trust and legal action.	High	High
R3	Further processing of data beyond original purpose	Discrimination, aggressive marketing	DPA Principle 2	Reputational damage, loss of public trust and legal action.	Medium	High
R4	Inaccurate / out-of-date data	Datastore compromised, privacy breaches, inaccurate identifications	DPA Principle 4	Reputational damage, loss of public trust and legal action.	Low	Medium
R5	Data being held longer than needed	Datastore compromised, privacy breaches.	DPA Principle 5	Legal action. Reputation damaged if deletion methods failing.	Low	Low
R6	Untimely or poor handling of SARs	Unable to access their own personal data	DPA Principle 6	Loss of public trust if SARs are regularly not handled properly, along with regulatory action	Low	Low
R7	Hacking of facial recognition images and MAC addresses	Identity theft	DPA Principle 7	Loss of public trust in the service, legal and regulatory action	Low	High
R8	Insider threats with regard datastore	Identity theft	DPA Principle 7	Loss of public trust in the service, legal and regulatory action, loss of sensitive corporate information	Low	High
R9	Non-EEA countries handling data	Identity theft	DPA Principle 8	Reputational damage, loss of public trust and legal action.	Low	High
R10	Discrimination through data sharing	Discrimination	HRA Article 14	Reputational damage, loss of public trust and legal action.	Low	High

R11	Personal data and communications interception and equipment interference	Data could be abused, loss of personal privacy	DIPB	Could be poor PR for BioConnect if this takes place in a specific investigation, as per the bill, and users did not know it was a possibility.	Low	Medium
R12	Mishandling of personal data	Various	EGDRP (from May 2018)	Large financial penalties, bad press.	Low	Medium
R13	Interception of personal data	Breach of personal privacy	Lawful Business Practice Regulation 2000	Negative press - better to inform users upfront this may happen rather than only make reasonable efforts at the last minute to inform them	Low	Medium
R14	Secure communications	Personal communications / information breached	PECR	Bad press, loss of faith in the service, regulatory action from the ICO	Low	Medium
R15	Individuals being identified in the background of surveillance images	Various	DPA	Some reputational damage, possible legal / regulatory action	Low	Low
R16	3rd party mishandling disclosures	Various	N/A	Bad press, PR, negative public perception	Low	Medium
R17	Unnecessary collection of MAC addresses as personal data	Unauthorised data processing	DPA Principle 3	Negative press if it was revealed this data was captured and not deleted promptly	Medium	High
R18	Installed camera placement	Overly intrusive	N/A	Bad public perception. Legal action unlikely unless cameras are placed in toilets.	Low	Low
R19	Unnecessary collection of sensitive pictures at home	Privacy intrusion	HRA Article 8	Legal action and loss of confidence from the public	Medium	High
R20	Criminals tracking users	Individual physical attack	N/A	Negative public reaction. This is unlikely to happen though and objectively could occur with or without BioConnect being used.	Low	Medium
R21	False positives and deliberately falsified facial images	Discrimination, embarrassment, identity theft	HRA Article 8	Reputational damage and major loss of faith in the system	Low	High
R22	MAC address spoofing by attackers	Identity theft, data compromised	DPA Article 7	Legal and regulatory action, loss of confidence in the system and attacks on the system like DDoS.	Low	High

Proposed Solutions

For each risk, a solution was proposed and these can be seen in Table 2 below. Each solution can be traced back to match against the original risk. Following ICO guidance, it is important our solutions adhere to Privacy by Design principles [17, 18], which we shall discuss next.

Table 2 – Proposed Solutions

Solution ID	Risk ID	Privacy Issue	Proposed Solution Details
S1	R1	Obtaining Explicit Consent / Awareness	Explicit consent must be sought via the device when a user first signs up. Be clear with the T&Cs and use a layered approach as suggested in [6] with users urged to read full terms and conditions available via a link. Also [16] suggests the use of QR codes to provide T&Cs and on the BioConnect website allow a user to enter their MAC address and upload a facial image as a form of authentication to be able to view, edit and delete information already stored on them. Also put up signs in the environment at entrances and re-inforce the message further in. [6] rightly states that using signs are important where people might not expect to be under surveillance.
S2	R2	Withdrawing Explicit Consent	Place a consent withdrawal mechanism on the same screen or page used to sign-up on the device. If this consent is withdrawn, all the data relating to that person is automatically deleted, apart from their internet browsing history which all CSPs in the UK are required to keep for 12 months as per [7] and [14].
S3	R3	Further processing of data beyond original purpose	Be vigilant with BioConnect clients, partners and resellers, possibly restrict territory sales. It is hard to picture this being a regular occurrence, so it is also something of an acceptable risk.
S4	R4	Inaccurate / out-of-date data	This can be dealt with in the main by digital forgetting or automatic deletion of records so any changes in device or appearance are handled on the next new sign-up. For specific problems the trained security team can be contacted by the user via email or a web form.
S5	R5	Data being held longer than needed	This is a difficult risk to remove completely. As a CSP, BioConnect have to keep internet browsing records for 12 months. At the time same, we do not want to keep MAC addresses or facial images any longer than is necessary. An automatic deletion policy for MAC addresses and facial images would likely contradict with the legal requirement to keep internet records. However, the MAC addresses gathered from Wi-Fi probe requests could be stored separately and then deleted daily. Recall user data must be deleted when consent is withdrawn though deleting all data would not be possible if the user has used the service to browse the web, as per the legal requirement already mentioned. The security team for this work have to be trained and reliable, with logging of deletions taking place.
S6	R6	Untimely or poor handling of SARs	The data controller's details need to be readily available to the user, with a team trained to handle SARs. The SARs themselves can be made via the website or in writing to the BioConnect headquarters. So we can explicitly put a link to a SAR form on the BioConnect website and direct people to it on printed material too.
S7	R7	Hacking of facial recognition images and MAC addresses	Use a secure tunnelled VPN in the network for transferring this data, encrypt the database using a sufficiently strong algorithm, and chose the best encryption method for the data itself when being transferred bearing in mind IoT power constraints. Invest time and effort upfront selecting IoT cameras (or even developing in-house) with enough embedded processing power and memory for secure encryption - amend the information flow so that images are only stored in IoT cameras in an encrypted format, not unencrypted, as this poses a vulnerability before transmission. Implement both secure cloud storage and secure physical storage, the choice will depend on the implementation. Consider empowering the user to choose storage option.
S8	R8	Insider threats with regard datastore	The security teams handling the data and the processes will be vetted, reliable and trained. Network access will be restricted with restrictions placed on hardware also, such as having no USB ports on the machines being used in a control room. Security measures like having no mobile devices or USB pens in the control room can be put in place. Monitor networks internally for suspicious insider threat activity and implement Role Based Access Control (RBAC). Implement a combined Intrusion Detection & Prevention System (IDPS).

S9	R9	Non-EEA countries handling data	For us to partner with one of these non EEA countries, we will seek impartial 3rd party legal advisors to work with both our legal team and that of the potential partners. If the law is not sufficiently strong in the potential territory, then it is best not to proceed with an arrangement.
S10	R10	Discrimination through data sharing	Article 14 of the HRA relates to prohibition of discrimination. Via sharing data with law enforcement or other agencies, this is a risk. This data sharing can take place in exceptional circumstances, such as matters of national security, or prevention of disorder or crime. We have to manage this process, be transparent and be vigilant that standards are being adhered to.
S11	R11	Personal data and communications interception and equipment interference	Be transparent. Mention in our terms & conditions very clearly that this may happen and we are legally obliged to assist authorities.
S12	R12	Mishandling of personal data	To comply with the forthcoming EGDRIP, make sure we have a data protection officer. Bear in mind a first written warning is provided before a penalty is imposed, so there is more margin for error to begin with as the regulation is implemented.
S13	R13	Interception of personal data	Make sure in the terms & conditions for users it is clear upfront this may happen, rather than only make reasonable efforts at the last minute to inform them.
S14	R14	Secure communications	Implement a breach log, make sure opting in is required as much as possible - that is, opted out should be a default stance ideally.
S15	R15	Individuals being identified in the background of surveillance images	Implementing face obscuring technology via a 3rd party is an option however it is considered minimal public intrusion to be in the background, given the nature of images posted on social media for example. It could also be costly. So, accept this risk.
S16	R16	3rd party mishandling disclosures	As part of the disclosure process, check the best practice of the 3rd party.
S17	R17	Unnecessary collection of MAC addresses as personal data	Set up a terminal at entrances to read the MAC address of a device and offer opt-in or opt-out of address collection. Explain clearly on signs this is to reduce data collection. Daily deletion of these basic Wi-Fi probe requests so data is not held unnecessarily.
S18	R18	Installed camera placement	Take care when designing system layout, conduct further consultations with stakeholders to define intrusive areas in each environment.
S19	R19	Unnecessary collection of sensitive pictures at home	Make sure home installations can be easily switched off by the user, and include some physical screen that can be opened and closed on home cameras.
S20	R20	Criminals tracking users	Have the client consider extra security personnel on the ground.
S21	R21	False positives and deliberately falsified facial images	Invest in high quality cameras and lighting, do not compromise, and make sure to set review dates for installations
S22	R22	MAC address spoofing by attackers	Ensure technical mitigation by checking new information against a stored profile to detect device changes relating to a MAC address.

Privacy by Design

The ICO states Privacy by Design is an approach to projects that promotes privacy and data protection compliance from the start. Although this approach is not a requirement of the DPA, it helps organisations comply with their obligations under the legislation [18]. This PIA document in an inherent part therefore of a Privacy by Design approach. There are seven core principles of Privacy by Design [17]. Here we list the principles and give examples of how the proposed solutions meet the principles:

1. Proactive not Reactive; Preventative not Remedial

As stated, this very PIA document is proactive as we wish to prevent risks from occurring rather than waiting until afterwards to deal with them.

2. Privacy as the Default Setting

BioConnect will require explicit consent to use the system. We strive to make sure every user's privacy remains intact if they do not give this explicit consent, for example by deleting records of Wi-Fi probe requests.

3. Privacy Embedded into Design

We do not wish to compromise or diminish functionality, privacy is integral to the system. BioConnect are prepared to invest time and effort into selecting the correct core components to adhere to this principle. For example, either choosing best-in-class IoT cameras for implementations, or shaping that landscape ourselves with our own in-house research and development into how to overcome IoT device resource constraints.

4. Full Functionality – Positive-Sum, not Zero-Sum

BioConnect will try to avoid unnecessary trade-offs between all affected parties. The classic example here is tackling the issue of keeping people secure versus collecting personal data with a view to achieving that exact purpose. They appear to be at odds with each other but by being thorough and carefully considering consultations, security and privacy do not need to be juxtaposed.

5. End-to-End Security – Full Lifecycle Protection

Our end-to-end protection starts with explicit consent being required, followed by data being securely encrypted and securely transferred to the datastore. This datastore is also secured and is only handled by suitable personnel. Deletion processes are maintained and logged to avoid storing data unnecessarily. We expect 3rd parties who request our data to uphold the same high standards.

6. Visibility and Transparency – Keep it Open

We will be clear in our T&Cs with what sensitive personal data is being processed, and why. This explanation includes the security and safety benefits as well as the legal requirements. We will also be upfront about stating in future we could be obliged to comply with investigations into matters of national security or crime.

7. Respect for User Privacy – Keep it User-Centric

Empowering users is important. Again, BioConnect does not compel users to use its Wi-Fi service. We strive to inform them of the service risks and policies through layered T&Cs and physical notices in their environment. This is key where users would not expect data to be collected and processed. With those purchasing implementations, we can give them recommendations and choices for how they wish data to be stored. Some small but important design aspects can be undertaken like physical shutters to cover a camera lens at home, making sure equipment can be turned off (Microsoft's Kinect IoT device received bad press in the past in this regard [19]) and not providing audio recording facilities [6].

Summary of Solutions

It is impossible to remove all risks in their entirety as no environment is risk-free. We are confident the solutions proposed are realistic in the whole however there is always the chance that an attacker may be more powerful than the IoT network itself and compromise it, or that they use that computing power to break any encryption on datastores.

IoT technology has not matured and there are vulnerabilities caused by resource constraints and a lack of standards compared to traditional IP. However, these risks are not insurmountable. Lightweight protocols, encryption methods and the correct selection of topologies contribute to adopting a best-in-class approach in line with the Privacy by Design principles, particularly numbers 3, 4 and 5.

False positives are always going to be a risk – 100% accuracy with biometrics is unattainable. Hence we recommend human involvement to handle mismatches as the system cannot be fully automated.

PIA Outcomes

With the potential scope of the system and its complexity, we propose that a robust sign-off procedure is adopted for both individual project implementations, and research and development. The Risk Register is a core part of this. Addressing risk, however, is a continual process and this register has to be maintained. We suggest scheduled bi-monthly reviews of each implementation and daily monitoring of industry press for zero-day threats that might affect our systems.

This PIA recommends that all of the solutions apart from S15 and S20 are implemented. S15 regards implementing face obscuring technology for background faces when capturing a foreground image but this is not essential and there is little difference between this and photos shared via social media. S20 relates to reducing actual physical harm to users via the client having an extra security presence – it is very likely that other physical threats that are outside of any made possible by using BioConnect have caused a suitable security presence on the ground to be set already.

When the risk register is studied there are a significant number of risks with high severity and low likelihood but nevertheless they cannot be ignored, hence our recommendation that the remainder of the solutions should be implemented. In conclusion, BioConnect can directly help deal with a number of society's security problems through technology - some of these solutions individually may be resource intensive or costly, but nevertheless, on balance when considering the whole solution and potential impact, these solutions and the project in the whole are worthy investments.

References

[1] ICO, “Conducting privacy impact assessments code of practice”, 20140225, v1.0, https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

[2] Human Rights Act 1998, http://www.legislation.gov.uk/ukpga/1998/42/section/14

[3] NHS Mansfield and Ashfield Clinical Commissioning Group, Newark and Sherwood Clinical Commissioning Group, “Privacy Impact Assessment (PIA)”, https://www.nottingham.ac.uk/emahsn/documents/stroke-edocument-data-sharing-privacy-impact-assessment.pdf

[4] ICO, “Determining what is personal data”, 20121212, v1.1, https://ico.org.uk/media/1554/determining-what-is-personal-data.pdf

[5] Data Protection Act 1998, http://www.legislation.gov.uk/ukpga/1998/29/contents

[6] ICO, “In the picture: A data protection code of practice for surveillance cameras and personal information”, 2015, v1.1, https://ico.org.uk/media/1542/cctv-code-of-practice.pdf

[7] Draft Investigatory Powers Bill, Nov 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf

[8] S. Carey, “Snooper’s Charter: What you need to know about the Investigatory Powers Bill”, ComputerWorld UK, 2nd Nov 2016, http://www.computerworlduk.com/security/draft-investigatory-powers-bill-what-you-need-know-3629116/

[9] Allen & Overy, “The EU General Data Protection Regulation”, 2016, http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf

[10] The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, http://www.legislation.gov.uk/uksi/2000/2699/pdfs/uksi_20002699_en.pdf

[11] Big Brother Watch, https://www.bigbrotherwatch.org.uk/about/

[12] Regulation of Investigatory Powers Act 2000, http://www.legislation.gov.uk/ukpga/2000/23/contents

[13] ICO, “What are PECR?”, https://ico.org.uk/for-organisations/guide-to-pecr/introduction/what-are-pecr/

[14] The Data Retention (EC Directive) Regulations 2009, http://www.legislation.gov.uk/uksi/2009/859/contents/made

[15] ICO, “In the picture: A data protection code of practice for surveillance cameras and personal information”, 2015, v1.1, https://ico.org.uk/media/1542/cctv-code-of-practice.pdf ***DUPE***

[16] ICO, “Wi-Fi location analytics”, 2016, v1.0, https://ico.org.uk/media/1560691/wi-fi-location-analytics-guidance.pdf

[17] Information and Privacy Commissioner of Ontario, “Privacy by Design”, Sept 2013, https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf

[18] ICO, “Privacy by design”, https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/

[19] H. Langley, “Microsoft explains why Xbox One Kinect isn’t a Prism spy tool”, TechRadar, 1st Nov 2013, http://www.techradar.com/news/gaming/consoles/microsoft-explains-why-xbox-one-kinect-isn-t-a-prism-spy-tool-1195705

[20] IEEE 802.11 standard, https://en.wikipedia.org/wiki/IEEE_802.11

Appendices

Appendix A – Stakeholder Questionnaires & Answers

Appendix A1 – Questionnaires sent out and responses received

Stakeholder 1 – you are a home-owning female parent, 40 years-old, with two children under the age of 10 years-old. You have various devices at home that could use this system though you are not particularly tech-savvy. Also, you use public transport regularly both on your own and sometimes bring your children. Please carefully consider the product information below, and then answer the questions. Thank you in advance!

BioConnect

BioConnect is a new product that uses a combination of facial recognition and a mobile phone MAC address tracking for authorising access to Wi-Fi. The system requires user consent to access the Wi-Fi unless they have already given their consent via previous use.

It is envisaged BioConnect is most beneficial in three main areas:

1. At home
2. On travel networks
3. In large public, private or hostile environments. For example, sports venues, office buildings or security situations respectively.

Example usage:

- in the home for controlled Wi-Fi access to prevent unauthorised use of devices, for example by children.
- in public places to reduce device theft and help catch thieves
- across a regional or international travel network incorporating subways, buses, train stations, airports and such like. It may be particularly useful for helping to secure large travel networks which may under terrorist threat, like the London Underground.
- locating individuals under some kind of time pressure, for example those who are late for a flight, or in more severe circumstances trying to pin-point terrorists inside a building where hostages are being held.
- in retail stores for tracking customer movements
- in buildings for tracking who in inside or outside
- for specific surveillance e.g. on travel networks, sports stadiums, entertainment parks, universities, schools, workplaces, supermarkets, conferences and events with controlled access, for example via turnstiles. This helps reduces risks of crime and terrorist attacks in venues and environments with a high density of people.

Functionality:

In order to join a Wi-Fi network, the system requires a picture of the user's face. The first time a user joins a network, this is stored with the MAC address of the device attempting to access the Wi-Fi in a central cloud-based datastore. Consider a MAC address to be a unique ID for each phone. Once a facial image and MAC address are recorded for a given device, the next time access is attempted, the image of the user must match the original capture. When a user returns to an environment where they have previously used the Wi-Fi and requests access once more, the system will check their face against the stored picture, and if the MAC address matches the stored MAC address, then Wi-Fi access will be granted.

In most cases it is thought the camera in the device attempting access will be used to take the picture. Alternatively, it can be taken via the installed cameras in the environment. For example, a camera in a user's house, or via a special kiosk camera in public, or cameras installed in the back of seats on a train. These cameras can be installed wherever the customer requests.

A user can leave a network and re-join it easily. An installed camera can automatically check the user's face and mobile phone MAC address when Wi-Fi access is requested, and if there is a match with the data already stored then access is granted.

In a home situation for example this prevents children using parent's devices. In other environments, if required, it is possible to alert an authority if a previously registered device attempts access and the image of the individual does not match that which is stored. This authority could be an on-site administrator, or a

security team. In environments where the datastore is shared with official security services, they can be notified also, for example if a known criminal or terror suspect is identified.

The system can track users in an environment via their phone's MAC address. People can also be tracked via their facial image. For example, in an airport if a connected device is stationary for an abnormal period of time, security can be notified and it can be investigated. The MAC address allows the specific model of device to be identified. For example, Samsung Galaxy Note 7 devices, which at time of writing are vulnerable to catching fire, have been banned by the US Department of Transportation from being carried onto a plane either in hand luggage or checked-in luggage.

Questions:

1. What activities do you use Wi-Fi for that you would consider to be sensitive or personal?

Sensitive activities which I would use Wi-Fi for are banking, sending messages using online apps, sharing photos with friends and browsing the internet.

2. What, if any, information would you be worried or uncomfortable about the system recording? Please describe what that information would be and why it would concern you.

I would be worried about the system tracking my location as I don't know who would have access to that and what it would be used for. I would not be comfortable using this system outside my home if it tracked my location. I also would not feel comfortable with this system storing pictures of me or my kids and would hate having a camera in the seat in front of me sending pictures to a server which people could access.

3. What concerns would you have over your children either intentionally or accidentally using the system at a) home b) in public?

A) I would not feel comfortable at all giving a system access to a camera in my home which would send pictures of to a server. The risk of sensitive pictures being sent is too high.

b) I would not feel comfortable with a system tracking my kids in public or taking pictures of them any time they access wifi.

4. Do you think having any age checking as part of the system would be valuable? For example, to make sure only over 18s were using the system.

No, I do not think blocking access to wifi based on age would be beneficial. I think for applying parental controls to internet access for kids the restriction would need to be more application specific as total ban on internet wouldn't solve anything.

5. In future would you be comfortable with any data being shared with other parties if we genuinely felt it would benefit you?

No I would not be comfortable with you sharing my data at your discretion. I would not feel comfortable with more data being connected than was necessary for authentication.

6. Even if you rarely or never used the service, how much would you care if it was installed in environments you travelled through?

I would not be comfortable with cameras being installed in public places for this system as I don't believe they would have enough oversight. I would be ok with the system being installed if it only used the device cameras or booths. The tacking system would also need approval before it logged any information.

7. Would how often you use the service affect how you felt about us storing your data? For example, visiting somewhere on a weekend break compared to passing through several train stations to and from work each day?

Yes I would be more willing to have some data stored if It made daily life better however I would not be as comfortable with places I don't often visit.

8. A cloud computing system stores information online instead of actually in a large computer in an office. How do you feel about your data being stored online in the cloud compared to on physical servers?

Stuart Millar 13616005

I feel that having my information in the cloud would make it less secure than it being in a specific office and also more accessible to people who wouldn't need access.

9. Tracking individuals and devices helps us identify people of interest, and devices that may be a threat. Would this tracking activity concern you, and if so why?

Yes, I don't think a private company who's purpose is to provide wifi access to be should have the capability or right to track peoples locations in public locations. If the system was in a private building and the tracking was optional then I think this feature would be ok.

10. To make system more secure we were considering asking for a user's date of birth and name as well on first registration so we can personalise the service. Would you be happy to provide these details to make the system more secure? Please discuss any concerns you might have also.

Yes I would be ok with sharing this information if it was stored securely. The main reason I do not disagree with this is that it is displayed publicly on social media and most websites ask for this information.

11. With this system it is possible your facial image may be recorded in the background when the system is analysing a person in the foreground. How would you feel about that?

I would be ok with this as long as these images aren't stored for longer than is necessary to analyse them and that they aren't shared. This is a daily occurs with selfies so that is why I would be ok with just their capture

12. Storing facial images and phone MAC address speeds up accessing Wi-Fi where this system is installed, as then a user doesn't need to provide a facial image each time. How long would you be happy for us to keep this data for before it is deleted?

I think for frequently accessed locations I think it should be a month after the last access request and for once off location I think it should be two weeks after last access request.

13. In certain circumstances we may need to share our data with the security services to help apprehend criminals. Would you have any concerns over this?

I would have concerns over the scale of the shared data. If data for a particular location and time and person this would be ok but not if sharing information on every customer was the practice for any request.

14. Would you have any physical privacy concerns using the system? Physical privacy risks are not those risks pertaining to your information, but those related directly to physical harm being caused to you.

I would have concerns with staff in your company having the ability to turn on cameras or track my location. I think this would be dangerous if a stalker other form on criminal managed to get access to your systems.

15. if we had a code of practice or terms, realistically would you read them? What would stop or discourage you from reading them?

They are typically very long and written using legal terminology which makes them hard to understand and so I would likely not read them. Also If I was connecting to wifi on the go I would likely not have the time to read these conditions.

Stakeholder 2 – you are a senior business executive that travels internationally daily by air and by train. When you travel you also use your laptop, tablet and mobile device for business use and personal use. Please carefully consider the product information below, and then answer the questions. Thank you in advance!

BioConnect

BioConnect is a new product that uses a combination of facial recognition and a mobile phone MAC address tracking for authorising access to Wi-Fi. The system requires user consent to access the Wi-Fi unless they have already given their consent via previous use.

It is envisaged BioConnect is most beneficial in three main areas:

1. At home
2. On travel networks
3. In large public, private or hostile environments. For example, sports venues, office buildings or security situations respectively.

Example usage:

- in the home for controlled Wi-Fi access to prevent unauthorised use of devices, for example by children.
- in public places to reduce device theft and help catch thieves
- across a regional or international travel network incorporating subways, buses, train stations, airports and such like. It may be particularly useful for helping to secure large travel networks which may under terrorist threat, like the London Underground.
- locating individuals under some kind of time pressure, for example those who are late for a flight, or in more severe circumstances trying to pin-point terrorists inside a building where hostages are being held.
- in retail stores for tracking customer movements
- in buildings for tracking who in inside or outside
- for specific surveillance e.g. on travel networks, sports stadiums, entertainment parks, universities, schools, workplaces, supermarkets, conferences and events with controlled access, for example via turnstiles. This helps reduces risks of crime and terrorist attacks in venues and environments with a high density of people.

Functionality:

In order to join a Wi-Fi network, the system requires a picture of the user's face. The first time a user joins a network, this is stored with the MAC address of the device attempting to access the Wi-Fi in a central cloud-based datastore. Consider a MAC address to be a unique ID for each phone. Once a facial image and MAC address are recorded for a given device, the next time access is attempted, the image of the user must match the original capture. When a user returns to an environment where they have previously used the Wi-Fi and requests access once more, the system will check their face against the stored picture, and if the MAC address matches the stored MAC address, then Wi-Fi access will be granted.

In most cases it is thought the camera in the device attempting access will be used to take the picture. Alternatively, it can be taken via the installed cameras in the environment. For example, a camera in a user's house, or via a special kiosk camera in public, or cameras installed in the back of seats on a train. These cameras can be installed wherever the customer requests.

A user can leave a network and re-join it easily. An installed camera can automatically check the user's face and mobile phone MAC address when Wi-Fi access is requested, and if there is a match with the data already stored then access is granted.

In a home situation for example this prevents children using parent's devices. In other environments, if required, it is possible to alert an authority if a previously registered device attempts access and the image of the individual does not match that which is stored. This authority could be an on-site administrator, or a security team. In environments where the datastore is shared with official security services, they can be notified also, for example if a known criminal or terror suspect is identified.

The system can track users in an environment via their phone's MAC address. People can also be tracked via their facial image. For example, in an airport if a connected device is stationary for an abnormal period of time, security can be notified and it can be investigated. The MAC address allows the specific model of device to be identified. For example, Samsung Galaxy Note 7 devices, which at time of writing are

vulnerable to catching fire, have been banned by the US Department of Transportation from being carried onto a plane either in hand luggage or checked-in luggage.

Questions:

1. What activities do you use Wi-Fi for that you would consider to be sensitive or personal?

I use Wi-Fi both at home and in public to both work and personal emails. The carry personal information like email address, phone number, name and address of both myself, colleagues and customers. Customer's information is particularly sensitive. The content of the emails may also be confidential. I also access my company's network via Wi-Fi, this involves lots of confidential information being sent and received.

2. How important is using Wi-Fi whilst you are away from your desk in your office, or when travelling?

It is of the upmost importance. I spend a lot of work time away from my desk and need to be able to communicate with colleagues and customers.

3. Some mobile phone devices may pose a problem, like those which can catch fire. Recently the Samsung Galaxy Note 7 was banned from all US flights as it was deemed to pose a danger. Would you want to know if someone had brought a banned model onto a plane? How would you feel about your device model information being stored?

I would want to know if someone brought a banned model onto a plane I was on. I would feel slightly uncomfortable but ok with it so long as it was just information on the phone model being stored. I would have concerns about other information being stored as well.

4. If you were a regular user of the system, say multiple times per day, how would you feel about explicitly giving consent to use the system every single time? For example, would having to provide a new picture every time be irritating?

Yes, once I am connected to a Wi-Fi, I should stay connected until I leave. I could tolerate providing a photo once per day but more than that seems excessive.

5. How important to you would it be to be able to access, edit or delete the information we store regarding you and your device?

It is important that the information be deleted if I request it. I would also want to be able to see what information is being stored about me and request that certain parts be deleted.

6. What, if any, information would you be worried or uncomfortable about the system recording? Please describe what that information would be and why it would concern you.

Email address, I get enough span email as it is. It also does not seem to be necessary for it to be stored.

Phone number, I get too many phone calls currently. It does not appear to be necessary for my phone number to be stored.

A history of places I have accessed the Wi-Fi. Sometimes I meet with potential clients before we have an official partnership. I would be uncomfortable with this information being made public.

7. Tracking individuals and devices helps us identify people of interest, and devices that may be a threat. Would this tracking activity concern you, and if so why?

Yes, as mentioned above I often need meetings with potential clients to be confidential.

8. What differences, if any, do you feel there are between using a chipped passport and facial recognition when you are travelling through an airport, and using our system for Wi-Fi access?

This system seems to extend beyond airports. However I do have similar concerns with regards to my movement being tracked.

9. To make system more secure we were considering asking for a user's date of birth and name as well on first registration so we can personalise the service. Would you be happy to provide these details to make the system more secure? Please discuss any concerns you might have also.

Stuart Millar 13616005

So long as a history of locations I have accessed the Wi-Fi is not being kept, I would have no problem with providing this information.

10. Would you feel safer in an airport knowing that we can investigate behaviour that seems out-of-the ordinary?

Yes, so long as tracking information is not being stored longer than necessary.

11. How concerned would you be about the possible collection of other data apart from your facial image and phone's MAC address as an unavoidable by-product of using the system? Presume this other data would simply be stored and not used for any other purpose.

Very concerned, as mentioned before I do not want my location history to be made public.

12. Storing facial images and phone MAC address speeds up accessing Wi-Fi where this system is installed, as then a user doesn't need to provide a facial image each time. How long would you be happy for us to keep this data for before it is deleted?

If I am using the service almost daily I would be comfortable with the images and MAC address being stored permanently, so long as no other information is also being stored.

13. Sharing the information we store could prevent terrorist attacks. Would you feel safer knowing that your travel route is being monitored for criminals and suspects?

So long as only people who the police have genuine reason to believe are terrorists are being monitored.

14. Generally, do you read terms and conditions of Wi-Fi or other digital online services you use? Please explain why you do, or why you don't.

No, I don't think it is important enough to spend the time.

15. And if we had a code of practice or terms, realistically would you read them? Again what would stop or discourage you from reading them?

I would probably not read them, I would likely be in a rush to get connected to the W-Fi.

Stakeholder 3 – you sit on the internal cyber security committee of BioConnect. You previously were an ethical hacker and worked as a contractor to strengthen vulnerable systems. From time to time you also appear as a guest in the media to discuss cyber security incidents. Please carefully consider the product information below, and then answer the questions. Thank you in advance!

BioConnect

BioConnect is a new product that uses a combination of facial recognition and a mobile phone MAC address tracking for authorising access to Wi-Fi. The system requires user consent to access the Wi-Fi unless they have already given their consent via previous use.

It is envisaged BioConnect is most beneficial in three main areas:

1. At home
2. On travel networks
3. In large public, private or hostile environments. For example, sports venues, office buildings or security situations respectively.

Example usage:

- in the home for controlled Wi-Fi access to prevent unauthorised use of devices, for example by children.
- in public places to reduce device theft and help catch thieves
- across a regional or international travel network incorporating subways, buses, train stations, airports and such like. It may be particularly useful for helping to secure large travel networks which may under terrorist threat, like the London Underground.
- locating individuals under some kind of time pressure, for example those who are late for a flight, or in more severe circumstances trying to pin-point terrorists inside a building where hostages are being held.
- in retail stores for tracking customer movements
- in buildings for tracking who in inside or outside
- for specific surveillance e.g. on travel networks, sports stadiums, entertainment parks, universities, schools, workplaces, supermarkets, conferences and events with controlled access, for example via turnstiles. This helps reduces risks of crime and terrorist attacks in venues and environments with a high density of people.

Functionality:

In order to join a Wi-Fi network, the system requires a picture of the user's face. The first time a user joins a network, this is stored with the MAC address of the device attempting to access the Wi-Fi in a central cloud-based datastore. Consider a MAC address to be a unique ID for each phone. Once a facial image and MAC address are recorded for a given device, the next time access is attempted, the image of the user must match the original capture. When a user returns to an environment where they have previously used the Wi-Fi and requests access once more, the system will check their face against the stored picture, and if the MAC address matches the stored MAC address, then Wi-Fi access will be granted.

In most cases it is thought the camera in the device attempting access will be used to take the picture. Alternatively, it can be taken via the installed cameras in the environment. For example, a camera in a user's house, or via a special kiosk camera in public, or cameras installed in the back of seats on a train. These cameras can be installed wherever the customer requests.

A user can leave a network and re-join it easily. An installed camera can automatically check the user's face and mobile phone MAC address when Wi-Fi access is requested, and if there is a match with the data already stored then access is granted.

In a home situation for example this prevents children using parent's devices. In other environments, if required, it is possible to alert an authority if a previously registered device attempts access and the image of the individual does not match that which is stored. This authority could be an on-site administrator, or a security team. In environments where the datastore is shared with official security services, they can be notified also, for example if a known criminal or terror suspect is identified.

The system can track users in an environment via their phone's MAC address. People can also be tracked via their facial image. For example, in an airport if a connected device is stationary for an abnormal period of time, security can be notified and it can be investigated. The MAC address allows the specific model of device to be identified. For example, Samsung Galaxy Note 7 devices, which at time of writing are

vulnerable to catching fire, have been banned by the US Department of Transportation from being carried onto a plane either in hand luggage or checked-in luggage.

Questions:

1. Do you think it is reasonable to ask a user to only provide their facial image to the system once on initial registration, and then again after some set time period has passed (like a few months), compared to asking them to provide a facial image every single time they wish to access the system?

In my opinion this would depend on how and where the system was implemented. For example in most cases providing a facial image every few months would be sufficient for most public venues, such as retail stores, universities and schools. However facial images should be more regularly required where controlled access is used (e.g. turnstiles). Facial images should be required most regularly in situations where the threat of terrorism is seen to be high, such as travel networks, including airports, international rail networks and city subways.

2. To make system more secure we were considering asking for a user's date of birth and name as well on first registration so we can personalise the service. Do you feel this data is commonly provided by the public already, and – if we decided to implement a requirement for a user's date of birth and name – would we be asking them to do anything they don't do already?

Again I feel that this may be subjective to how and where the system is implemented, however considering the user is willing to provide a facial image there may be fewer objections to providing this additional information. In cases where free service is provided (e.g. free internet access) most users will provide this information.

3. From the description of the system, and your own experience, please describe any vulnerabilities you feel might exist. For example, in relation to the cameras we might use, the collection process of the facial images, the MAC addresses, and also how they are stored.

One of my main concerns regarding this system would be its accuracy and how effectively it could identify falsified facial images. For this reason I would recommend high quality cameras in the IoT devices, this may be more difficult to manage however, where identification of users is carried out with personal mobile devices, where variation in camera sensors can be significant. Another concern would be the possible spoofing of MAC addresses on mobile devices, which when paired with a falsified facial image could provide a false identity for the user. Storage of personal data including names and dates of birth along with Images and MAC addresses should always be a primary concern for those implementing this system, and every possible measure should be taken to prevent the theft of this data.

4. We are aware that it can be difficult to encrypt data being transmitted over IoT as it uses constrained devices with little memory and CPU power. Should we be concerned about this, and can you make any recommendations in this area?

This should be a major concern for those adopting this system, especially when it is being implemented in a public place, including transport infrastructure, sports venues, schools, universities and retail complexes. This issue has the potential to allow attackers to intercept unencrypted communications which would contain personal data. My recommendation regarding this would be to invest in more powerful IoT devices for implementations where security is paramount, including transport infrastructure (e.g. airports and subways etc.) allowing strong encryption methods to be used. For instances where security is not as critical, a solution may be to utilise lightweight encryption methods for the devices.

5. We expect users will want to know about how data can be protected in case it falls into the wrong hands or is leaked. In your experience does this happen regularly, and can you suggest any mitigations?

In my experience, situations such as this occur on a regular basis, however in most cases the information has not been handled correctly or sufficiently protected. I would suggest that measures be taken to both protect data against external threats (system hardening, data encryption etc.) and internal threats with implementation of RBAC. This will decrease the likelihood that personal data stored by the system can be divulged by an unauthorised user.

6. Is there any way we could protect the data so it could not be read or used if it was leaked?

Yes – To ensure the data cannot be read if a breach occurs it should be stored in an encrypted database, various different standards exist which could provide acceptable levels of protection for stored data. Data should also be encrypted during transmission to ensure that intercepted data cannot be read if intercepted, I would also recommend ensuring that all network application layers are also encrypted as standard.

7. Should we be concerned about using cloud storage instead of on-site physical servers?

The use of cloud storage can spark many concerns regarding the privacy and security of user data. These can include threats from attacks against the service provider, threat of data released by disgruntled employees etc. However these fears can be addressed by encrypting the data using encryption keys unknown by the data host, therefore ensuring the data is not viewable by their employees. If BioConnect intends to roll out their product on a large scale it may be worthwhile investing in their own cloud infrastructure therefore giving them more control over their data.

8. Are there any advantages / disadvantages to user data being stored in the cloud compared to physical servers?

There are various advantages and disadvantages in utilising cloud based storage over on-site servers. One such disadvantage of cloud storage is that a measure of control over the data is relinquished when using a cloud hosted solution, and this can lead to threats such as the ones mentioned in Q7. However cloud storage can provide greater efficiency and availability to the customer organisations using the BioConnect system than an on-site server could. This would lead me to believe that it would be more practical to implement a cloud based solution providing sufficient security measures were put in place.

9. We still have to fully consider how long we are storing customer data for. What thoughts do you have with regard what is reasonable?

In my opinion BioConnect should adhere as closely as possible to the Data Protection Act of 1998 when forming the policies surrounding customer data storage. I would recommend consulting with a lawyer to address the finer points of this, and to prepare for any imminent changes which may occur to this legislation.

Stakeholder 4 – you are a 23-year-old tech savvy university student living in London. You are something of a fair-weather protester with regard to privacy and human rights but they are still important to you, and you attend rallies when you can. You've been the victim of phone theft in the past and your parents were caught up in the London Underground bombing in 2005, although they were not harmed. Please carefully consider the product information below, and then answer the questions. Thank you in advance!

BioConnect

BioConnect is a new product that uses a combination of facial recognition and a mobile phone MAC address tracking for authorising access to Wi-Fi. The system requires user consent to access the Wi-Fi unless they have already given their consent via previous use.

It is envisaged BioConnect is most beneficial in three main areas:

1. At home
2. On travel networks
3. In large public, private or hostile environments. For example, sports venues, office buildings or security situations respectively.

Example usage:

- in the home for controlled Wi-Fi access to prevent unauthorised use of devices, for example by children.
- in public places to reduce device theft and help catch thieves
- across a regional or international travel network incorporating subways, buses, train stations, airports and such like. It may be particularly useful for helping to secure large travel networks which may under terrorist threat, like the London Underground.
- locating individuals under some kind of time pressure, for example those who are late for a flight, or in more severe circumstances trying to pin-point terrorists inside a building where hostages are being held.
- in retail stores for tracking customer movements
- in buildings for tracking who in inside or outside
- for specific surveillance e.g. on travel networks, sports stadiums, entertainment parks, universities, schools, workplaces, supermarkets, conferences and events with controlled access, for example via turnstiles. This helps reduces risks of crime and terrorist attacks in venues and environments with a high density of people.

Functionality:

In order to join a Wi-Fi network, the system requires a picture of the user's face. The first time a user joins a network, this is stored with the MAC address of the device attempting to access the Wi-Fi in a central cloud-based datastore. Consider a MAC address to be a unique ID for each phone. Once a facial image and MAC address are recorded for a given device, the next time access is attempted, the image of the user must match the original capture. When a user returns to an environment where they have previously used the Wi-Fi and requests access once more, the system will check their face against the stored picture, and if the MAC address matches the stored MAC address, then Wi-Fi access will be granted.

In most cases it is thought the camera in the device attempting access will be used to take the picture. Alternatively, it can be taken via the installed cameras in the environment. For example, a camera in a user's house, or via a special kiosk camera in public, or cameras installed in the back of seats on a train. These cameras can be installed wherever the customer requests.

A user can leave a network and re-join it easily. An installed camera can automatically check the user's face and mobile phone MAC address when Wi-Fi access is requested, and if there is a match with the data already stored then access is granted.

In a home situation for example this prevents children using parent's devices. In other environments, if required, it is possible to alert an authority if a previously registered device attempts access and the image of the individual does not match that which is stored. This authority could be an on-site administrator, or a security team. In environments where the datastore is shared with official security services, they can be notified also, for example if a known criminal or terror suspect is identified.

The system can track users in an environment via their phone's MAC address. People can also be tracked via their facial image. For example, in an airport if a connected device is stationary for an abnormal period of time, security can be notified and it can be investigated. The MAC address allows the specific model of

device to be identified. For example, Samsung Galaxy Note 7 devices, which at time of writing are vulnerable to catching fire, have been banned by the US Department of Transportation from being carried onto a plane either in hand luggage or checked-in luggage.

Questions:

1. Do you feel this system differs in any way from traditional CCTV systems? If you do, please explain why.

Yes as the CCTV system will not be able to identify you automatically against the MAC address. This system would be able to detect you personally.

2. How concerned would you be about the possible collection of other data apart from your facial image and phone's MAC address as an unavoidable by-product of using the system? Presume this other data would simply be stored and not used for any other purpose.

I would be concerned on what information is stored and if it is personally sensitive. I would like if this information would be disclosed. I would not be concerned as much if it is know that this information is not being used.

3. Do you think collecting facial images and MAC addresses is sensitive data, compared to, say, your home address or your bank details? Explain your answer.

I believe that any collection of information that together can be used to identify a person is sensitive information. Even though other information described above could be even more sensitive.

4. How important to you would it be to be able to access, edit or delete the information we store regarding you and your device?

Very important. Being able to delete the information is a right that all data subjects should have as circumstances and viewpoints change.

5. With this system it is possible your facial image may be recorded in the background when the system is analysing a person in the foreground. How would you feel about that?

I feel that there should be some method of blurring on background people to allow for some privacy of people captured. For example if a face is recognised the system could blur any other faces it recognises before it is saved.

6. What, if any, information would you be worried about the system recording? Please describe what that information would be and why it would concern you.

I would be worried about the system storing location information as I would be uncomfortable if the system was able to track or predict where I was going at any given point.

7. Tracking individuals and devices helps us identify people of interest, and devices that may be a threat. In certain circumstances we may need to share our data with the security services to apprehend criminals. Would this tracking activity concern you, and if so why?

I would be concerned in the case of how accurately the system can recognise a face. For example if I look like a known criminal but am not that person will it flag up a response from security personal? Also as stated above I would be concerned of any tracking facilities this software had

8. Some mobile phone devices may pose a problem, like those which can catch fire. Recently the Samsung Galaxy Note 7 was banned from all US flights as it was deemed to pose a danger by catching fire. Would you want to know if someone had brought a banned model onto a plane? How would you feel about your device model information being stored?

I believe that this information would be relevant in stopping potential threats. I don't think phone information should be stored but rather have the capability of checking the model against a list of vulnerable devices. If it does match a vulnerable model then a flag could be placed on the MAC address or information stored.

9. How do you think you would react if the system mistook you for someone else by accident and you could not access Wi-Fi, or if you were mistaken for a person who the authorities wanted to speak to?

Stuart Millar 13616005

I would question the effectiveness of the system as a whole. I know that people can look similar but certain methods may be put in place. For example, if you are blocked from the Wi-Fi this could be disclosed and allow you to verify that you are a different person. I understand if it is an investigation this information must be kept secret and I would be deeply upset if the security forces accidently mistook me for a criminal.

10. Storing facial images and phone MAC address speeds up accessing Wi-Fi where this system is installed, as then a user doesn't need to provide a facial image each time. How long would you be happy for us to keep this data for before it is deleted?

I believe that maybe a period of 6 months would be appropriate to ask a user if they wish to update the information, keep the information the same or delete the data the system has stored on them.

12. Sharing the information we store could prevent terrorist attacks. Would you feel safer knowing that your travel route is being monitored for criminals and suspects?

I don't agree to the information being shared, but I think this could be alleviated by allowing faces of known criminals to be put onto the system to allow for identification without sharing all the information to security forces.

13. How do you feel about your data being stored online in the cloud compared to on physical servers?

I would be happier for cloud based servers as I think their security would be greater than that of a local server.

14. How anonymous would you feel using the system as described? Can you suggest anything that would make you feel more anonymous?

I wouldn't feel too anonymous as if the information was leaked or an insider threat was using the information for their own benefit they would be able to identify a vast amount of people. I believe that if the developers disclosed their policies in training staff, updating and correctness of data stored and how they ensure the data is secured it would help people feel this information they share will allow them to remain anonymous in practice.

15. To make system more secure we were considering asking for a user's date of birth and name as well on first registration so we can personalise the service. Would you be happy to provide these details to make the system more secure? Please discuss any concerns you might have also. 1,2,3,4

I feel that storing this information is not what the product was designed to do. I believe this is not needed to provide the services described above, i.e. allow for Wi-Fi access. Even though having the mac address and photograph of the user is personal information if the system is compromised it may still be difficult for the hacker to determine the names and address of these people. While if this information is provide it could leave them at a greater risk.

Appendix A2 – Responses given to others

Product Overview

This app will use encryption to allow users to send text bases messages anonymously and privately. The message will be encrypted on the sender's device using public key private key encryption methods. It is then sent to our server where it is stored and sent on to the recipient. It is then decrypted only when the message is opened. The user has the option of protecting the app using one of the following methods:

- PIN
- Password
- On screen pattern
- Facial recognition
- Fingerprint (if the hardware allows)

Facial recognition and fingerprint data will only be stored on the users device and will be encrypted. There will also be optional two-factor authentication that can be used in conjunction with one or more of the above methods. It comes in the form of a token generating a 6-didget code on the push of a button.

The app will have two modes, a 'private' mode and a 'private and anonymous' mode. In the former, the users account will be tied to their phone number, this means that other people will only need their phone number to be able to send them a message. In 'private and anonymous' mode, each user will have a unique identification number that can be used to send them a message.

Stakeholder Profile

You are the company's Data Protection Officer (DPO). You are quite technically literate and personally very concerned with the privacy of the users of the app.

Questions

1. Do you see any breaches or potential breaches in the Data Protection Act or any other legislation in the app described above?

   There are a number of points I would make here. Strictly speaking we aren't collecting the facial recognition data and the fingerprint data if they are only being stored on the user device. However, if we are assigning users a unique identification number we should be careful. If these are assigned by us to users then we are holding personal data, as that ID can be used to identify a user. Give some thought to when we are assigning those IDs - are we are only assigning those unique IDs to users when they first use the 'private and anonymous mode' (i.e. they may never have unique ID if they never use that mode), or are we assigning those unique IDs to everyone who uses the app, regardless if they use that mode or not. Either way it needs to be made very clear to the user that we are assigning or may assign them a unique ID which we can identify them by.

   We need to define how long the encrypted messages are kept on our servers and what happens if the message is not delivered for some reason. It is mentioned that it is stored but there needs to be more detail on that from user's point of view.

Principle 7 of the Data Protection Act (DPA) concerns information security, stating:
"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

If per chance the data is decrypted, and that data is sensitive, such as their religious beliefs or info regarding their physical or mental health, we may be open to action being taken against us, even if we are following encryption guidelines from the likes of the ICO. I am not aware of a concrete legal definition of "appropriate" as above and there is always the chance a jury would say the encryption and other technical measures we might take are not "appropriate".

We also need to be careful that this app is not used for assisted in committed any offences under the Computer Misuse Act. The Computer Misuse Offences are:

1. Unauthorised access to computer material.
2. Unauthorised access with intent to commit or facilitate commission of further offences.
3. Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.
3A. Making, supplying or obtaining articles for use in offence under section 1 or 3.

If we study part 3A closely:

3A. Making, supplying or obtaining articles for use in offence under section 1 or 3 -

(1) A person is guilty of an offence if he makes, adapts, supplies or offers to supply any article intending it to be used to commit, or to assist in the commission of, an offence under section 1 or 3.
(2) A person is guilty of an offence if he supplies or offers to supply any article believing that it is likely to be used to commit, or to assist in the commission of, an offence under section 1 or 3.
(3) A person is guilty of an offence if he obtains any article with a view to its being supplied for use to commit, or to assist in the commission of, an offence under section 1 or 3.
(4) In this section "article" includes any program or data held in electronic form.

Can I draw your attention to part (2) in italics above. We need to decide if we believe the app is likely to be used to assist the commission of an offence under the Computer Misuse Act. There are two questions in this stakeholder document relating to criminal behavior so perhaps you and your team have begun to think about this already and I would urge to you to continue to consider it seriously.

There is a General Data Protection Regulation that was agreed in April 2016, this will come into force in two years on May 2018 across Europe – despite Brexit we need to be ready for that too even though it is not an immediate concern, and I would recommend your team are familiar with that also. Our legal partners, Allen & Overy, sent me this guide: http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf. For example, as per that regulation, where personal data is processed for direct marketing the data subject will have a right to object. This right will have to be explicitly brought to a user's attention.

Lastly we will need to seek further legal advice for the other parts of the world that this app might be rolled out in. I am not aware of all the legislation in each territory and the legislation which we adhere to in the UK could conflict with that of other countries but what I can say is there are embargos in place for certain countries and in theory we could be breaking those if we are selling the app in restricted areas.

2. If the user's anonymity was compromised, how do you think public reaction to this would impact the company?

   I think there could be a scandal, given that is one of the inherent key features provided by using the app. This would hold true for a normal member of the public and in additoin if a person in the security services, public eye or political arena was revealed to be using the app then there might be pressure as to why, and lead to questions or pressure on us regarding what was in the content of the messages. Any public scandal would affect our reputation, which we can't measure the cost of, our customer's trust and we could suffer financial penalties too if we are found to be breaking the law.

3. If the user's private messages where compromised, how do you think public reaction to this would impact the company?

   If the content was scandalous then we would be under pressure for having facilitated the sending of these messages. Even if the content was not scandalous then we would be under pressure as if one set of messages were compromised, the question would be asked how soon could others be compromised. In the former case, we would be scrutinised regarding whether or not we knew what the content of the messages were, and pleading ignorance will not cut it, if for example terrorists were exchanging messages and we in theory could have decrypted those messages if we wanted to. The argument would then be our lack of action in this area could indirectly be helping criminals. At the same time the value proposition is that the messages are only decrypted once the receiving user opens then, so our teams do not know what the messages are at any point. A key question here is whether our teams do not or should not know what the messages are. Can we get the content of the messages if we want to? We could be accused of assisting offenders and ethically that is hard to defend and would damage our reputation, even if our terms & conditions and DPA provisions were watertight.

4. If a user's facial recognition or fingerprint data was successfully extracted from a lost or stolen device, how do you think public reaction to this would impact the company?

   Again the reaction would not be favourable though I would assert a number of other companies with apps on the phone could be compromised at the same time, so the focus may not solely be on our app. Still, we should always consider the worst case scenario. Whilst we would not be collecting this data ourselves per se, if it goes no further than the user phone, it would indicate a vulnerability in the application which, rightly or wrongly, may be considered by our customers to stretch to other applications we develop too. The public perception is important here even if legally there are no issues.

5. Is there any personal information that you think customers would be uncomfortable with us keeping?

   There will be concerns I am sure about the possibility of personal information being contained within the encrypted messages that are stored on our servers. Being transparent and gaining

consent is important, we have to give customers the choice. If they aren't totally comfortable with this then they have the choice obviously not to use the app in the first place. Location data is increasingly sensitive so if we are capturing that to analyse where the app is being used then we need to take care and again explain explicitly that this is happening. If the app is a paid for "as-a-service" then I think keeping customer details and bank details is reasonable as long as it is secured, in fact it is likely going to be required for the project to be financially feasible.

6. Anonymous metadata regarding how many people are using the app and what parts of the world the app is popular in may be kept for our own marketing purposes. Do you foresee any problems or scandals arising because of this?

   It depends how exactly we are gathering the data and if the end results are anonymized, or if the users are truly anonymous during the metadata gathering. If we are simply counting the number of users without identifying them during that count then I do not see any problem in that specific case. If individually identifying each user is an unavoidable part during the process of checking which parts of the world the app is popular in, even if we are only using the aggregate anonymous data for marketing, then we need make users aware this is happening and give them the option to opt-in, not opt-out. We shouldn't be gathering location information by default – customers should be choosing to opt-in to that, I can't stress this enough. The temptation may be there in the marketing department to use the individual's location data eventually for targeted marketing specific to that individual. The public bristle at the thought of any idea of tracking and targeting that may be happening to them, or could happen to them in future without their knowledge. We need to make the user aware that this data may be kept for our own marketing purposes, it has to be specifically stated to them that this may happen, and they have to agree to it.

   This anonymous metadata can be considered a residual risk of encrypted data transfer, for example if it stored in an unencrypted form which is then the target of an attack. If our implementation relies on public-key infrastructure, then I assert it must implement strict certificate checking to maintain trust in end-points. This is a useful guide from the ICO: https://ico.org.uk/for-organisations/guide-to-data-protection/encryption/data-transfer/

   As outlined above it sounds like there could be some form of tracking taking place if we are able to determine where someone is using the app. There have been numerous cases, e.g. with the Snowden leaks, showing that this metadata can be used to build up a picture of which unique user IDs are talking to each other, how many messages they are sending, when they are sending the messages and where in the world they are. We need to consider this carefully. If we get a Freedom of Information request asking for location data we could be in trouble if we haven't been transparent with users that this is happening. The same applies for a Subject Access Request asking about what data we hold and why hold it – if that shows the geographical data gained via some sort of tracking, and users are not aware of this, then that could trigger a scandal.

7. Do you have any concerns over the apps potential to be used for criminal activity and what implementations that might have for the reputation of the company?

   Yes, for sure. Criminals want their communication to be secret and it could be said an encrypted messaging app would be attractive to them. For this reason, we need to tread carefully, we do not want to be seen to be supporting criminals if they use our app and then publicise that use, or somehow recommend our app to others. We have to be whiter-than-white and for good reason to protect our user's privacy. If authorities request access to the encrypted messages or user details then we would be in a very difficult position, akin to that which Apple faced when the FBI wanted information on a phone found after the San Bernardino shooting. Do we relinquish the privacy

aspect the app is founded on, or not? As a DPO I would say yes but naturally I cannot speak for the whole company and it depends on the context.

8. Do you think we have any obligation to monitor potential criminal use?

   We aren't legally obliged I don't think but if anything suspicious seems to be taking place then we have to report it to the relevant authorities. And as I've explained above, if we are deemed to be helping an attacker commit an offence under the Computer Misuse Act, I would be worried about hindsight showing us the whole thing could've been avoided if we were monitoring the app properly for criminal use. We could consider including a statement regarding monitoring in the terms of use for the app though I understand this is at odds with the total privacy the angle is trying to achieve. Also, again bear in mind we might be asked to provide the decryption key by a UK court if there is a criminal investigation, for example if a phone is acquired by the police.

9. Is there anything else, not outlined above, that you foresee being a potential problem or scandal?

   I think this app is a solid technical idea though pushes the ethical and legal boundaries compared to our standard messaging products. I would urge caution again. Some final points:

   - in the documentation for the app if it goes live eventually please make sure I am identified as the Data Protection Officer so I can handle relevant queries and issues for you.

   - consider where the messages are stored i.e. on a physical server only we can access that is under lock and key, versus secure storage in the cloud.

   - bear in mind the potential use of the app by those under 18.

   - presuming we are charging for this service, we need to consider the collection of bank details, billing addresses etc. And it follows we will have their name also. All the data then becomes personal data as we can link it to an individual. Even if we don't have their name the other data is still enough to identify the individual if we have this unique ID, which is obviously for ID purposes. We are going to have a listing, somewhere, of unique IDs matched against phone numbers. If this is the case, we need to handle all of this as personal data as this processing falls within the scope of the DPA. We have to be careful about the type of encryption used and the details of that as if that information is compromised then those messages could be decrypted with enough computing power.

   - consider if we also store the PIN, password and on-screen pattern on our side, this isn't mentioned in the product overview.

Privacy Impact Assessment Consultation Questionnaire

Company Background

We are a medium sized logistics company with between 200-300 staff. Every employee in the organisation, including C level executives, department heads and low level staff, have been provided with a corporate email account. The organisation has an IT department of 8 members who are responsible for the operation, administration and maintenance of infrastructure including mail servers. The R&D department are responsible for the developing of a new system with the purpose of reducing the number of phishing emails arriving in employee mailboxes.

Your role

You are an external shareholder of the company on the board of directors. Your opinion is vital for this privacy impact assessment as you may be required to react in the event of a scandal. As an important stakeholder in the company your opinions will weigh heavily on the decisions taken in development.

System overview

The new email security system will analyse all incoming and outgoing emails in order to detect potential phishing scams. This will be achieved by analysis of the metadata, headers, and body of each email against signatures of known suspicious communications. The system will also incorporate sophisticated analysis of attachments to reduce the number of malicious files received by employees. Suspicious communications will be quarantined and stored until reviewed by a system administrator (member of IT). Due to the nature of the system it is unlikely to be 100 percent accurate and false positive may occur. As the system is in the early stages of development it has not been decided whether the solution will be hosted locally or cloud based.

Q1. Do you think that it is acceptable to implement a system which scans every incoming and outgoing corporate email for the purposes of reducing the likelihood of a breach caused by a phishing attack?

Yes, absolutely. These attacks are so common, and many do not make the news. Our company is of the typical size which are targeted by hackers as they feel we will not have security measures like you describe. We do need to take care though that the team monitoring the communications has the correct training and we have to make sure all the staff are aware that the monitoring is taking place, and why we are doing it. As an external shareholder I don't want my return on investment harmed either by a scandal being triggered.

Q2. The new email system will likely store suspicious employee emails for a period of time until reviewed by a system admin, which may lead to the disclosure of employee personal information to these members of staff. Please indicate your concerns regarding this.

1. How long are these emails stored for exactly, where are they stored and how secure are they.

2. After they have been reviewed, they should be deleted once no longer needed – will this be the case?

3. I would be concerned about a member of the IT staff reading emails with the sensitive personal information of others. This is difficult to manage as I appreciate we need to do this, and this is the first time we are introducing it. That said, might I suggest staff should only use corporate email for corporate use, that way the chances of that happening are greatly reduced.

4. I'm not comfortable with how that responsibility for reading sensitive emails is delegated, it seems too simple for me.

Q3. Have you any opinions on strategies which could be implemented to minimise the exposure of emails containing personal information?

I think it is very important as few people have access to them as possible, and that they are securely stored so that they cannot be compromised and leaked to others.

Q4. Do you think that additional training of administrators of the new system in the handling of personal information would be beneficial in avoiding potential scandal?

Yes, this is essential I think, though the effectiveness of the training depends on selecting the right people to train in the first place. If we have unreliable people reviewing these emails then they could steal personal information, or leak commercially sensitive business information to the press. I gather the Data Protection Act requires us to take steps to ensure reliability of any staff who have access to personal data. I don't want my emails being reviewed by a bunch of amateurs.

Q5. Do you think that a change in company policy regarding the transmission of personal data by employees would be beneficial in avoiding potential scandal? Please explain.

Yes, we need to make them aware we are doing this, and changing company policy to state, for example, that personal data should not be transmitted by corporate email, is a good idea. The wording used in the company policy and the reasons for it need explained clearly to all staff, or else the change in company policy in itself could lead to a scandal if it arouses suspicion, even if we have everyone's best interests at heart.

Q6. In your opinion what would be the most effective way of notifying staff regarding the new system to minimise possible outrage at privacy violation.

We need to highlight the fact we as a company face a threat by hackers from phishing attacks, and the damage this can cause, such as if we are blackmailed. Then we can explain as a preventative measure we are considering developing this new system, and consult with the staff to take their concerns into consideration as well. We should do this in person with everyone and then make a record that they have been informed for completeness, but also hold review sessions, say every 6 months. We should explain what the system does and does not do. If we hide anything from the staff this could trigger a scandal if we haven't been honest with them.

Q7. Developers of the system are assessing the merits of a cloud based solution which would mean that the processing of employee emails would be carried out externally. Please indicate your concerns regarding privacy in this matter.

I would be concerned regarding how we control the data they are looking at, how long they are keeping it for and their deletion policies. We would have to trust an external third party not to mishandle this information – for example passing company information to the press - and also trust that their security systems and storage systems are strong enough to withstand attacks. If all our email communication is to be directed to this external company then we expose ourselves to significantly higher risk than if we keep everything in-house in my opinion.

Q8. In your opinion what are the privacy implications of inspecting every attachment which travels through our mail server?

I can understand the need for attachment inspection to check if they contain viruses and so on that could damage the company. At the same time inspecting every single attachment sounds excessive, surely out of 10,000 attachments maybe only one or two are suspect? For example, could it be argued if an email is exchanged between two people within the organisation, and the content seems perfectly reasonable, then there is no need to check any attachments? Then again there is the argument that the attachments need to be inspected in any event – the phishing attacks are getting so complex these days, especially with social

engineering where attackers could be impersonating our employees and encouraging them to open attachments that may seem innocent, like invoices or word documents, when in fact they are malicious.

Q9. Can you think of any other scenario leading to scandal which may arise because of the proposed new system?

You correctly mention false positives. I think mistakenly identifying someone as some sort of suspect or highlighting someone (or some email) for blame could cause problems for us, for example if a member of staff felt discriminated against or ostracised for opening a malicious attachment. I wouldn't that happening to me, as an external shareholder I have invested in this business for the long-term.

Q10. Can you think of any additional measures which could be taken to avoid scandal due to a breach of privacy caused by the new system?

The legislation needs checked thoroughly, particularly the Data Protection Act, to ensure we are compliant if this new system is implemented.

Thank you for your feedback.

Privacy Impact Assessment Questionnaire – Customer

Product Overview:

This product is used in conjunction with online sales websites, i.e. amazon, eBay, and it will monitor purchases made by customers in order to suggest additional products that may benefit from being used with the purchase. Details held in the system include: Card details, name, and delivery address. The product will also monitor transaction details to try detect fraudulent activity on the account and help mitigate from this.

Stake Holder Profile:

You are a 30-40 year old Father of two teenage kids. You are of average technology awareness but have been targeted by fraudsters in the past that cost you >£1000 of damages from credit card fraud so is sceptical of releasing card details. All members of the family commonly use web services to purchase items.

Questions:

Do you think this service is different from other what current occurs on sites like eBay? If yes, explain how?

From what is explained above, I don't think so on first impression. When I have used eBay to buy products for myself and my children I regularly am recommended other products to be used with the purchase. eBay stores the same details as described above too. What I am not sure about is what the relationship between the selling site and the product, mainly who does the actual recommending (the site or your company making the product), and who stores my personal data (again the site, or the company making the product). I have been targeted in the past so I am wary of this.

What type of information would you be willing to release to the system? I.e. Name, address etc.

I understand for ordering items, giving my name and address are reasonable expectations. My credit card details are needed to make purchases, I understand that – but I am not sure I would be comfortable releasing credit card details to a 3rd party company working in conjunction with a selling site.

Is there any information you would be uncomfortable to release to the system?

As above – I would be wary of giving my credit card details to a 3rd party that wasn't the site itself as I have been targeted by fraudsters in the past. I would not really be keen for the location of my purchase to be recorded by the system, nor those of my family.

Are there any reasons why you may wish to hide your purchases from someone? I.e. your family, friends etc.

Not that I can think of, though if I was buying gifts for my kids for Christmas I would not want them stumbling across those details. I don't see why my purchases should not be hidden as a default to be honest.

Are there any products that you think may be too sensitive for the system to take record off?

I would not be happy with the product recording products that might reveal information about my or my family's physical or mental health, for example if they were buying medical products or resources.

Do you have any concerns about how the data may be handled within the system?

Yes, since I have been targeted in the past I would want significant reassurances about how well my personal data is secured, where is stored, who has access to it and how long it is kept for. Sometimes 3rd parties sell data onto other companies too and I do not want to be hassled in this manner.

Would you object to members of the Fraud detection team being able to extract your transaction information from the system?

I would want to know that your fraud detection team had been trained properly and that they were reliable people, not a bunch of part-timers. I would object in the first instance unless you could prove this to me somehow when I signed up to use the service.

Would you have any reason for you to ask the developers to release your information from the system?

Yes I am a firm believer that I should be able to access any data you hold on me. So the very fact I am asking should be reason enough and I would like to know the process for this before I used the product. If by 'release' you mean delete then yes if I was no longer using the product I would want all my data deleted, and in any event I would not want my data held for any longer than was necessary. I don't see why this data would still be held if I wasn't using the system or had used it for a period of time.

How likely is it that another person my use your details to purchase an item online? I.e. a family member or friend.

It is very likely, I let my wife use my account to keep things simple. I wouldn't let a friend use it though. She is my wife obviously so it is different for her using my account compared to a friend but I am not sure I would want her to be able to see all the products I had bought in the past, in case some were presents for her, or for some other reason. My privacy is my privacy at the end of the day and no-one else's.

How many locations would you have as a delivery address for transactions?

I can think of two, my house and my office at work. Though I am thinking about only having things delivered to my house in future as I've heard about systems being compromised and the delivery address being changed to other people in other countries.

PRIVACY IMPACT ASSEMENT QUESTIONNAIRE

Stakeholder Profile

Data protection officer: you are the data protection officer for a company intending to use this system. You will be in charge of managing this software and performing initial reviews on any flagged items. You will also be responsible for its implementation and for the storage of personal data which is collected. You have been asked in the past to help in internal investigation will be asked to use this software in the future to investigate employees for not following code of conduct or other minor productivity issues.

Product Overview

Functionality

This is a workplace monitoring software for use in organisation to improve productivity and to perform investigations into staff for insider threats and offences under the code of conduct. The software has a number of features including email monitoring, internet monitoring, file tracking and internal communication monitoring. The software also offers configurability based on employee access level and other characteristics.

The software will monitor emails, recording the subject, date and time of employee's emails. The software can be set up to flag keywords in the content of emails which will alert the system admin and require review of email content to decide whether or not this is a valid concern. The keywords which are searched for are set by the system admin to fit the company's needs and extra search words can be added to particular employees which are suspected of breaking contract or code of conduct. The software will also monitor all outgoing email attachments for detection information leaks. Similar monitoring features will be implemented to monitor internal communication.

The software will log all internet traffic, storing the time and date, user location, and sites visited. The software will not store search terms or keystrokes and will not log what pages are visited on a site. The system admin can set a list of restricted sites which if visited will flag that the user has visited the site.

The software also logs employee file access and can flag when a user accesses a file which would not be needed for their role. The software will also monitor any coping of files to removable media or to online services.

Implementation and policies

The software can be set up to know employee access rights to prevent false positives and also logging features can be reduced at certain times of the day or if a device is not on the organisations network (i.e. personal device at home). The data collected by the system is available to all the senior IT personnel and all managers can access data on the staff they supervise. The data will be retained until the admin of the software feels it is no longer relevant.

There will be full disclosure to staff about data retention policies, management policies and monitoring activity at the start of employment with reminder sent yearly. Staff will be notified of any widespread changes to the policies except for cases of individual investigation where monitoring can be increased without notification. Keywords used will not be disclosed so as to maintain effectiveness.

Questions

Please answer questions bellow in text boxes. Feel free to increase their size if necessary. Thank you in advance for your participation.

Question 1: Have you any concerns about sensitive person data (i.e. data that can be used to discriminate) being collected by this system?

The DPA principles state personal data shall be not be excessive and it sounds like what we are monitoring might be over the top. We need to make sure if we go ahead with this we are only holding as little information as possible to achieve what we want to – can't we just block the sites we don't want people to access instead of tracking them like this? I do not think the assigning of keywords to flag a review of email content should be set by a system admin, especially if that privilege is abused. I'd suggest some sort of working group to do this requiring a layer or two of sign-off from management. The system admin deciding when the data will be deleted is also cause for concern, for example if they forget to delete it and the data store is compromised, or again if a system admin keeps emails and personal data for malicious use. It sounds like logging features may have to be manually reduced for devices leaving the network and I am definitely not comfortable with that. If this is the case we run the risk of intentionally or unintentionally logging activity to the same degree outside the office as inside the office and

Question 2: Do you think this is an acceptable level of monitoring for web browsing?

I am still coming to terms with this – if we have to protect from insider threats then we have to be able to make sure employees aren't triggering some sort of attacks via visiting malicious websites that might infect our network. That is the reality. That said, for those not up to speed on the reasons for this web browsing, it might not be acceptable. We need to make sure we are transparent and very clear for our reasons for doing this.

Question 3: Have you any concerns with automatic scanning of emails for key words and flagging findings to admin staff?

Yes, again I am not comfortable with the admin staff having responsibility for setting the filters. We would like to think this would not be abused but it is this type of filter misuse that can trigger a scandal. Who monitors the monitors, if you follow me? i.e. who is checking the admin staff? We need to be on top of this if it is implemented, they can't be left to their own devices.

Question 4: Do you agree with the frequency of notification to staff about the monitoring?

No in fact I think it should be at least quarterly. Perhaps the development team could build-in an on-screen notice every time a user logs in, that way they we would be issuing a reminder daily. It could be too much though, people may be immune to it eventually, so maybe once a week or once a fortnight is better. We could set up a consultation group with the staff about

Question 5: Have you any concerns with monitoring internal communications for key words?

Yes, it could be open to abuse and inappropriate key words could be used. Again this comes back to exactly what type of filtering is being done. We can't afford for commercially sensitive information to be gathered and potentially be made available to outside parties, and of course our staff might consider this to be very intrusive. Corporate email is not meant to be for personal use but we need to be realistic that is not adhered to 100% of the time.

Question 6: Have you any concerns over the availability of the data collected by the monitoring software and who can access it?

I am not comfortable with all managers having access to data on the staff they supervise. In theory they could access the sensitive personal data being collected and discriminate or ostracize staff, or at least the staff could make those sorts of claims. It is important for people handling that sort of data to be trained in doing so, and also be reliable in the first instance. I can't say right now if all our senior IT personnel and all managers are suitable or not, we need to find this out. The data should be available to as few people as possible and I think this is too wide a group of people.

Question 7: Have you any concerns over potential abuse of the automated systems?

Yes we are open to that happening sadly. I would like to think it wouldn't happen but it is a possibility, so the correct checks and controls have to be in place. I don't feel giving all the responsibility to our system admin is the right way to do it, it needs to be some sort of group consensus, and there needs to be a check on the how the automated systems are being used. In fact might I suggest I am directly involved in that group to offer guidance and protect us from scandal.

Question 8: Is the data retention policy acceptable to prevent holding irrelevant information?

I would assert not – we need to be more specific about how long we are holding information for, and when it is being deleted. Transparency here will appease the concerns of the staff.

Question 9: Can you identify any issues which could cause scandal for the company if publically released?

I think I've outlined several above – my feeling is that the monitoring may be excessive and I think the number of people with access to the data is too large, this logically increases the chances of a scandal if there a more potential points for information to be leaked. If a system admin was abusing the system to gather personal data and the public was made aware of this, it would trigger a scandal for sure. If we wrongly suspect someone of wrong doing, that is also bad for the company's reputation. Monitoring workplace productivity using this tool sounds too authoritarian I have to say – surely there are other ways to boost productivity than this? We don't want a reputation for micro-managing people.

Question 10: Have you any other privacy concerns or legal concerns in regards to data protection?

We need to give more thought to how this fits in with the Data Protection Act. We could take a softer approach and insist on consent from an individual but then we couldn't compel them to do that, and if they don't consent where does that leave them in terms of their specific role? Alternatively, there is a condition of data processing that states the processing has to be in accordance with a "legitimate interest" condition. I think we could say protecting ourselves from insider threats and so on is a legitimate interest though we should double-check this. In that situation, we would not need the explicit consent of all staff but I would strongly recommend that just as much effort is put in with regard to making them aware of what is being proposed or it could backfire and trigger a scandal.

Appendix B – Data Protection Act 1998 – the eight Principles plus Schedule 2 and 3

SCHEDULE 1

The data protection principles

Part I

The principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—
(a) at least one of the conditions in Schedule 2 is met, and
(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

SCHEDULE 2

Conditions relevant for purposes of the first principle: processing of any personal data

1. The data subject has given his consent to the processing.

2. The processing is necessary—
(a) for the performance of a contract to which the data subject is a party, or
(b) for the taking of steps at the request of the data subject with a view to entering into a contract.

3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4. The processing is necessary in order to protect the vital interests of the data subject.

5. The processing is necessary—
(a) for the administration of justice,
(b) for the exercise of any functions conferred on any person by or under any enactment,
(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
(d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

6.—(1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.
(2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

SCHEDULE 3

Conditions relevant for purposes of the first principle: processing of sensitive personal data

1. The data subject has given his explicit consent to the processing of the personal data.

2.—(1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.
(2) The Secretary of State may by order—
(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
(b) provide that, in such cases as may be specified, the condition in subparagraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

3. The processing is necessary—
(a) in order to protect the vital interests of the data subject or another person, in a case where—
(i) consent cannot be given by or on behalf of the data subject, or
(ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or
(b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4. The processing—
(a) is carried out in the course of its legitimate activities by any body or association which—
(i) is not established or conducted for profit, and
(ii) exists for political, philosophical, religious or trade-union purposes,
(b) is carried out with appropriate safeguards for the rights and freedoms of data subjects,
(c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and
(d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6. The processing—
(a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
(b) is necessary for the purpose of obtaining legal advice, or
(c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7.—(1) The processing is necessary—
(a) for the administration of justice,
(b) for the exercise of any functions conferred on any person by or under an enactment, or
(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.
(2) The Secretary of State may by order—
(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or
(b) provide that, in such cases as may be specified, the condition in subparagraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

8.—(1) The processing is necessary for medical purposes and is undertaken by—
(a) a health professional, or
(b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.
(2) In this paragraph “medical purposes” includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9.—(1) The processing—
(a) is of sensitive personal data consisting of information as to racial or ethnic origin,
(b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and
(c) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

(2) The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.
10. The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.